UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,109	12/20/2001	Donald P. Matthews JR.	BRCMP016/BP2009	7508

7590 03/14/2005

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 03/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/026,109	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *December 20, 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/28/02,1/21/03*. 8/28/03
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 5-9, 11-13, 17-21, 23-24, 31-32, 36-37 and 44-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Matthews, Jr. United States Letter Patent Number 6,549,622.

As per claim 1:

Matthews teaches a cryptography accelerator for generating a stream cipher, the cryptography accelerator comprising:

a key stream generation core for performing key stream generation operations; (Col. 2, lines 51-53; Col. 3, lines 1-3; Col. 7, lines 1-2)

a memory associated with the key stream generation core, the memory including a plurality of input ports configured to obtain write data associated with a stream cipher

and a plurality of output ports configured to provide read data associated with the stream cipher, wherein the key stream generation core and the memory are operable for performing a plurality of read data operations and a plurality of write data operations associated with generating the stream cipher in a single cycle. (Col. 2, lines 56-62; Col. 3, lines 4-6; Col. 4, lines 27-29; Col. 7, lines 2-7)

As per claim 5 and 17:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator wherein the stream cipher is associated with three variables. (Col. 11, lines 38-39 and lines 59-61)

As per claim 6 and 18:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator wherein a read operation and a write operation are performed using a first variable and the memory in a first cycle. (Col. 12, lines 22-25)

As per claim 7 and 19:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory wherein a read operation and a write operation are performed using a second variable and the memory in a second cycle. (Col. 12, lines 26-27 and lines 38-42)

As per claim 8 and 20:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory wherein a read

operation and a write operation are performed using a third variable and the memory in a third cycle. (Col. 12, lines 43-57)

As per claim 9 and 21:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory wherein the stream cipher is ARC4. (Col. 2, lines 2-4; Col. 7, lines 7-8; *ARC4 is interpreted as RC4, the interpretation is given based on the description given of the disclosure*)

As per claim 11 and 23:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further discloses a cryptographic accelerator and a memory comprising a plurality of byte flops. (Figure 8A, items 808, 810, 812)

As per claim 12:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further disclose a cryptographic accelerator wherein the key stream generation core is operable to perform key shuffle operations and key stream generation operations. (Col. 2, lines 51-53; Col. 3, lines 1-3; Col. 7, lines 1-2; Col. 11, lines 54-57; Col. 12, lines 43-58)

As per claim 13:

Matthews teaches a memory associated with a cryptography engine for generating a stream cipher, the memory comprising:

a plurality of input ports configured to obtain write data associated with generating a stream cipher; (Figure 6; Col. 2, lines 56-62; Col. 3, lines 4-6; Col. 4, lines 27-29; Col. 7, lines 2-7)

a plurality of output ports configured to provide read data associated with the stream cipher, wherein a plurality of read data operations and the plurality of write data operations associated with generating the stream cipher are performed in a single cycle. (Figure 6; Col. 2, lines 56-62; Col. 3, lines 4-6; Col. 4, lines 27-29; Col. 7, lines 2-7)

As per claim 24:

Matthews teaches a method for pipelined generation of a key stream byte, the method comprising:

incrementing a first address during a first clock cycle; (Col. 3, line 11; Col. 12, lines 14-57)

reading a first memory value at the first address, reading a second memory value at the second address obtained by adding the memory value at the first address to a previous second address, writing the first memory value to the second address and the second memory value to the first address, and summing the first and second memory values to yield a third address during a second clock cycle; (Col. 3, lines 12-16; Col. 12, lines 14-57)

reading a third memory value at the third address during a third clock cycle. (Col. 3, line 16; Col. 12, lines 14-57)

As per claim 31:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further disclose a method comprising providing the third memory value as a key stream byte. (Col. 3, lines 18-19)

As per claim 32:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further disclose a method wherein the key stream byte is an ARC4 key stream byte. (Col. 2, lines 2-4; Col. 7, lines 7-8)

As per claim 36:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further disclose a method wherein the key stream byte is associated with the generation of a multibyte ARC4 key for decrypting a data stream. (Col. 2, lines 2-4 and lines 56-64; Col. 7, lines 7-8)

As per claim 37:

Matthews teaches a cryptography accelerator for pipelined generation of a key stream byte, the cryptography accelerator comprising:

means for incrementing a first address during a first clock cycle; (Col. 3, line 11; Col. 12, lines 14-57)

means for reading a first memory value at the first address, reading a second memory value at the second address obtained by adding the memory value at the first address to a previous second address, writing the first memory value to the second address and the second memory value to the first address, and summing the first and

second memory values to yield a third address during a second clock cycle; (Col. 3, lines 12-16; Col. 12, lines 14-57)

means for reading a third memory value at the third address during a third clock cycle. (Col. 3, line 16; Col. 12, lines 14-57)

As per claim 44:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further disclose a cryptography accelerator comprising means for providing the third memory value as a key stream byte. (Col. 3, lines 18-19)

As per claim 45:

Matthews teaches all the subject matter as discussed above. In addition, Matthews further disclose a cryptography accelerator wherein the key stream byte is an ARC4 key stream byte. (Col. 2, lines 2-4; Col. 7, lines 7-8)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2-3 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews, Jr. United States Letter Patent Number 6,549,622 in view of Kundarewich et al. Title "A CPLD-based RC4 cracking system" (Pages 397-402).

As per claim 2 and 14:

Matthews teaches a key stream generation core using a fast hardware implementation of the RC4 algorithm. Matthews does not explicitly disclose a cryptography accelerator wherein generation of the stream cipher is pipelined using coherency checking.

Kundarewich et al. in analogous art however, disclose generation of the stream cipher that is pipelined using coherency checking. (Page 398, col. 2, paragraph 2 ; ...the order of the two writes is done to preserve the coherence of data...)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include generation of the stream cipher that is pipelined using coherency checking. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Kundarewich et al. (Page 398, paragraph 2) in order to perform read and write at the same clock cycle.

As per claim 3 and 15:

Matthews teaches a key stream generation core using a fast hardware implementation of the RC4 algorithm. Matthews does not explicitly disclose a cryptography accelerator wherein the coherency checking comprises determining whether a write address is the same as a read address in a single cycle.

Kundarewich et al. in analogous art however, disclose a coherency checking comprising determining whether a write address is the same as a read address in a

single cycle. (Page 398, col. 2, paragraphs 2 and 3; ...CPLD supports only a single read or write access... an extra clock cycle is not necessary....)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include a coherency checking comprising determining whether a write address is the same as a read address in a single cycle. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Kundarewich et al. (Page 398, paragraph 2) in order to perform read and write at the same clock cycle.

6. Claims 4, 16 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews, Jr. United States Letter Patent Number 6,549,622 in view of Kundarewich et al. Title "A CPLD-based RC4 cracking system" (Pages 397-402) further in view of Correale, Jr. United States Letter Patent Number 4,998,221.

As per claim 4, 16 and 27:

Matthews and Kundarewich et al. teach all the subject matter as discussed above. Both references do not explicitly disclose a cryptography accelerator wherein a read operation bypasses the memory when the write address is the same as the read address.

Correale in analogous art however, disclose a read operation that bypasses the memory when the write address is the same as the read address. (Col. 3, lines 8-28; Col. 4, lines 7-9)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews and Kunarewich et al. to include a read operation that bypasses the memory when the write address is the same as the read address. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Correale (Abstract) in order shorten the time required to perform a write and read operation.

7. Claims 10, 22 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews, Jr. United States Letter Patent Number 6,549,622 in view of Schneier "Applied Cryptography" (Page 397-398)

As per claim 10, 22 and 33-34:

Matthews teaches a key stream generation core using a fast hardware implementation of the RC4 algorithm. Matthews does not explicitly disclose a cryptographic accelerator wherein the memory is initialized in a single cycle.

Schneier in analogous art however, disclose a cryptographic accelerator wherein the memory is initialized in a single cycle. (Page 397, line 23; ...initializing the S-box and fill it linearly)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include a cryptographic accelerator wherein the memory is initialized in a single cycle. This modification would have been obvious because a person having ordinary skill in

the art would have been motivated to do so, as suggested by, Schneier (Page 397) in order to provide a faster encryption.

As per claim 35:

Matthews and Schneier teach all the subject matter as discussed above. In addition, Matthews further discloses a method wherein the key stream byte is associated with the generation of a multibyte ARC4 key for encrypting a data stream. (Col. 2, lines 2-4 and lines 56-64; Col. 7, lines 7-8)

8. Claims 25-26, 28-30, 38-39 and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews, Jr. United States Letter Patent Number 6,549,622 in view Koppala United States Letter Patent Number 6,289,418.

As per claim 25 and 38:

Matthews teaches a key stream generation core using a fast hardware implementation of the RC4 algorithm. Matthews does not explicitly disclose a method comprising performing read-after-write coherency checking.

Koppala in analogous art, however, disclose a method of comprising comprising performing read-after-write coherency checking. (Col. 4, lines 55-58)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include comprising performing read-after-write coherency checking. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Koppala (Abstract) in order to accelerate data retrieval and storage.

As per claim 26 and 39:

Matthews and Koppala teach all the subject matter as discussed above. In addition, Koppala further discloses a method wherein read-after-write coherency checking comprises determining whether a first memory value at a first address is being read and written in the same clock cycle. (Col. 14, lines 59-63)

As per claim 28 and 41:

Matthews teaches a key stream generation core using a fast hardware implementation of the RC4 algorithm. Matthews does not explicitly disclose a method of comprising performing write-after-write coherency checking.

Koppala in analogous art, however, disclose a method of comprising performing write-after-write coherency checking. (Col. 4, lines 55-58)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews to include performing write-after-write coherency checking. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Koppala (Abstract) in order to accelerate data retrieval and storage.

As per claim 29 and 42:

Matthews and Koppala teach all the subject matter as discussed above. In addition, Koppala further discloses a method wherein write-after-write coherency checking comprises determining whether a first address is being written to twice in the same clock cycle. (Col. 14, lines 59-63)

As per claim 30 and 43:

Matthews and Koppala teach all the subject matter as discussed above. In addition, Koppala further discloses a method wherein a single write is performed if it is determined that a first address is being written to twice. (Col. 14, lines 59-67 and Col. 15, lines 1-6)

9. Claims 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews, Jr. United States Letter Patent Number 6,549,622 in view of Koppala United States Letter Patent Number 6,289,418 and further in view of Correale, Jr. United States Letter Patent Number 4,998,221.

As per claim 40:

Matthews and Koppala teach all the subject matter as discussed above. Both references do not explicitly disclose a cryptography accelerator wherein the given memory value is bypassed by a read operation if the first address is being read and written in the same clock cycle.

Correale in analogous art however, disclose a cryptography accelerator wherein the given memory value is bypassed by a read operation if the first address is being read and written in the same clock cycle. (Col. 3, lines 8-28; Col. 4, lines 7-9)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Matthews and Koppala to include a cryptography accelerator wherein the given memory value is bypassed by a read operation if the first address is being read and written in the same clock cycle. This modification would have been obvious because a person having

ordinary skill in the art would have been motivated to do so, as suggested by, Correale (Abstract) in order shorten the time required to perform a write and read operation.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
Examiner
Art Unit 2133

03/04/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100